Solution Brief

Netskope Zero Trust Data Protection

Netskope Zero Trust Data Protection brings best-in-class Data Loss Prevention (DLP) together with innovative technologies like machine learning and User and Entity Behavior Analytics (UEBA) onto a converged Security Service Edge (SSE) platform for context-aware access to data based on zero trust principles across web, cloud, email, private apps, and endpoints.

Quick Glance

- Greater visibility and risk mitigation across all key vectors from a single converged Security Service Edge (SSE) data protection solution
- Simplified data classification, policy definition, and incident management, driven by machine learning and advanced analytics
- End-user agility and reduced friction with flexible context-driven policies and a lightweight agent

"With Netskope we're seeing a paradigm shift in terms of DLP usability. We simply turn on the tool, watch the traffic, and adjust where needed. The system automatically suggests data to protect, meaning we can get on with defining alerts and policies rather than categorizing data."

Information Security Manager,
Australian Healthcare Provider

The Challenge

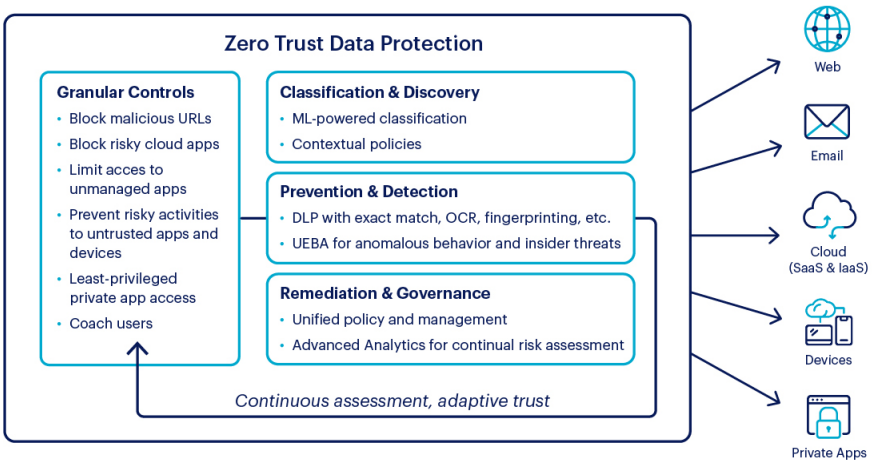
Existing enterprise security and data protection strategies have been disrupted by ongoing cloud adoption, the hybrid work model, and exponential growth in the amount of data created, captured, or replicated. To control and protect data while complying with global data privacy regulations, organizations must address the following:

- How can we detect and classify sensitive data, while gaining insights into its usage as it traverses the network, web, cloud, email, private apps, and devices?
- Does the data comply with our organizational security, policy, and compliance requirements?
- How can we resolve incidents and ensure policies are continually updated to keep up with growing and evolving data protection challenges?

In parallel to these ongoing data protection challenges has been recognition that the "implicit trust" inherent to traditional security controls is no longer applicable for hybrid work environments.

The Solution

Netskope Zero Trust Data Protection eliminates implicit trust and enables context-driven, least privileged access to data while continuously evaluating and adjusting the access levels to prevent user over-entitlement. This provides organizations with granular visibility and control over data. Additionally, the solution utilizes machine learning and Advanced Analytics to simplify data classification and policy definition, respectively, rapidly accelerating time to deployment and reducing ongoing operating costs.



Risk visibility and mitigation

In the current hybrid world, where users have the flexibility of accessing data and collaborating from any managed or unmanaged devices and from any location, data protection solutions must move from implicit trust-based controls to dynamic, context-driven controls. Additionally, the data protection solutions must extend their coverage from enterprise perimeters out to the web, cloud, private apps, and endpoints to close all the security gaps across key exfiltration points.

Netskope Zero Trust Data Protection leverages zero trust principles and state-of-the-art data protection controls in a single converged Security Service Edge (SSE) platform for enabling deep visibility into data usage and mitigating risks across the business footprint. Key capabilities include:

- Granular access controls to block malicious websites and risky cloud apps, limiting data access via unmanaged apps and behaviors, and coaching users
- Sophisticated DLP functionality like exact data matching and fingerprinting
- User and Entity Behavior Analytics (UEBA) to identify user behavior anomalies and insider threats that evade detection by conventional technologies
- Unified data protection across web, SaaS, IaaS, email, private apps, and devices to eliminate coverage gaps and enable incident correlation for greater efficacy
- Zero trust principles that enable context-based, granular, least-privileged data access, along with continuous assessment that dynamically adapts access based on changing context

Platform consolidation to reduce complexity

Organizations depending on a mix of point security solutions for securing data across different vectors often end up with complex deployments, resulting in inconsistent data visibility and protection, policy duplication, and remediation via multiple consoles.

Netskope Zero Trust Data Protection dramatically simplifies data classification, policy definition, and incident management with a converged platform, further aided by machine learning, rich reporting, and Advanced Analytics. The key capabilities include:

- Converged data protection and incident management across web, SaaS, IaaS, email, private apps, and devices to eliminate the need for multiple siloed data protection solutions and policies
- Machine-learning-enhanced data classification to automate large parts of the data classification process, reducing the need for organizations to commit to months-long classification projects before deploying DLP
- Advanced Analytics to enable organizations to gain insights into their data for identifying key risk areas or priorities and tailoring their policies accordingly

Improved user experience

In most organizations, the end-user experience gets compromised due to highly restrictive data and application access policies, as well as the installation of performance-intensive agents on their devices that significantly impact productivity.

Netskope Zero Trust Data Protection boosts end-user agility and reduces friction with flexible context-driven policies that allow users the freedom to access data and apps commensurate to the risk, and a lightweight agent that causes minimal impact on the user experience.

The key capabilities include:

- Contextual policies and coaching enable organizations to grant risk-appropriate access to apps and data
- Lightweight unified agent with cloud-based inspection minimizes the impact of DLP on the user experience

Why Netskope?

Truly converged single-pass data protection across all vectors: While some security vendors may offer unified policy and management, they either don't cover all the vectors (on-premises data centers, SaaS, IaaS, email, etc.) or integrate disparate point solutions with multiple management consoles. Netskope provides coverage across all the vectors and simplifies operations with a unified single-pass architecture and a single management console.

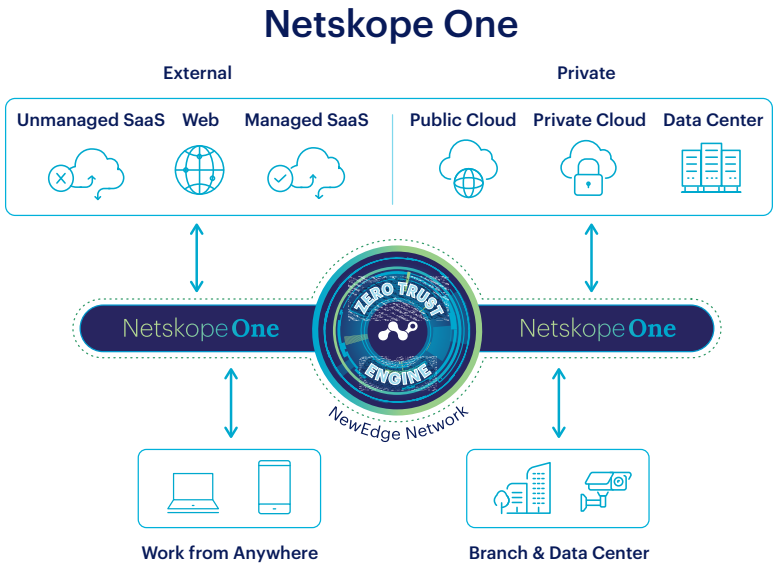
Contextual policies: Netskope Intelligent SSE's Business Transaction Analysis (CloudXD) and Zero Trust Engine are able to provide an exceptional degree of risk context around data—including identity, device, behavior, browser, location, activity, and threat—as well as where it is going. This results in an unmatched level of visibility that enables organizations to make better risk-based decisions with greater security and more flexible user experiences than what other more limited data protection offerings can offer.

ML-enhanced data classification: While many competitive DLP solutions require extensive data classification projects before they can become fully operational, Netskope's machine-learning capabilities help to automatically identify and classify data, enabling customers to accelerate their DLP deployments with minimal delays.

Use of UEBA to identify insider threats: Conventional DLP solutions utilizing traditional capabilities like RegEx and standard rules-based inspection have a very difficult time identifying data incidents committed by "insiders." Netskope uses UEBA to identify anomalies and correlate seemingly benign actions by insiders that can constitute data exfiltration or unauthorized use.

Advanced Analytics: Advanced Analytics is a unique solution offered by Netskope that helps organizations understand and communicate risk associated with cloud and web use, data protection, and cybersecurity threats. This is especially useful for data protection, as organizations can leverage the insights gained from Advanced Analytics to identify key gaps or areas for improvement, which can be automatically translated into policy.

Lightweight agent with cloud-based inspection: Netskope leverages a single agent for delivering endpoint DLP as well as securing access to the web and cloud. This agent is especially lightweight, as almost all security inspection happens in the cloud—other vendor solutions typically require one or more thick clients, and endpoint DLP inspection in particular is very resource-intensive, dramatically impacting the user experience.



What can you achieve with Zero Trust Data Protection?

Zero Trust Data Protection is delivered via Netskope Intelligent SSE, a converged cloud security platform that protects against advanced and cloud-enabled threats and safeguards data across all vectors (any cloud, any app, any user). A single-pass architecture delivers a fast user experience and simplified operations.

BENEFITS	DESCRIPTION
CONSOLIDATION	Consolidate protection strategies across all data types in all locations by eliminating redundant overlapping tools.
EFFICACY	Increase efficacy and reduce attack surfaces by applying zero trust principles enhanced with continuous, adaptive, context-aware, least-privileged access.
OPERATIONAL EFFICIENCY	Streamline security operations by implementing machine-learning-based classification and analytics-driven dynamic policy construction.
USER EXPERIENCE	Deliver a superior user experience by balancing trust against risk, providing the right level of access at the right time for the right reasons.